



Identity Theft:

Consumer Education, Business
Practices and Law Enforcement
Tools

June 2006

Questions to Make You Think

- ◆ Do you place your outgoing mail in your mailbox and then put the flag up?
- ◆ Do you carry your SSN card in your wallet or purse?
- ◆ Is your SSN your Driver's License Number?
- ◆ Do you shred?
- ◆ Do you receive pre-approved credit card offers that you don't want?
- ◆ Do you have passwords on your accounts?

What is Identity Theft?

- ◆ When someone else uses your personally identifying information without your knowledge or permission to:
 - Obtain Credit Cards in your name or makes charges on your existing accounts
 - Obtain Wireless or phone products, services
 - Obtain personal, student, car and mortgage loans, or cashes convenience checks, in your name
 - Obtain Employment

Other Uses of your Personal Information

- ◆ Commit crimes in your name
- ◆ Get medical services in your name
- ◆ Get Internet services or sends emails in your name
- ◆ Lease an apartment or house in your name
- ◆ File bankruptcy in your name

Techniques Identity Thieves Use to Get Information

- ◆ Dumpster Diving
- ◆ Shoulder Surfing
- ◆ Breaking & Entry
- ◆ Bribing or inserting corrupt employees
 - Steal files
 - Run unauthorized credit checks
- ◆ Skimming
- ◆ Hacking
- ◆ Pretexting
 - ❖ Credit reports
 - ❖ Solicitations
 - ❖ Web sites
- ◆ Phishing

Dumpster Diving



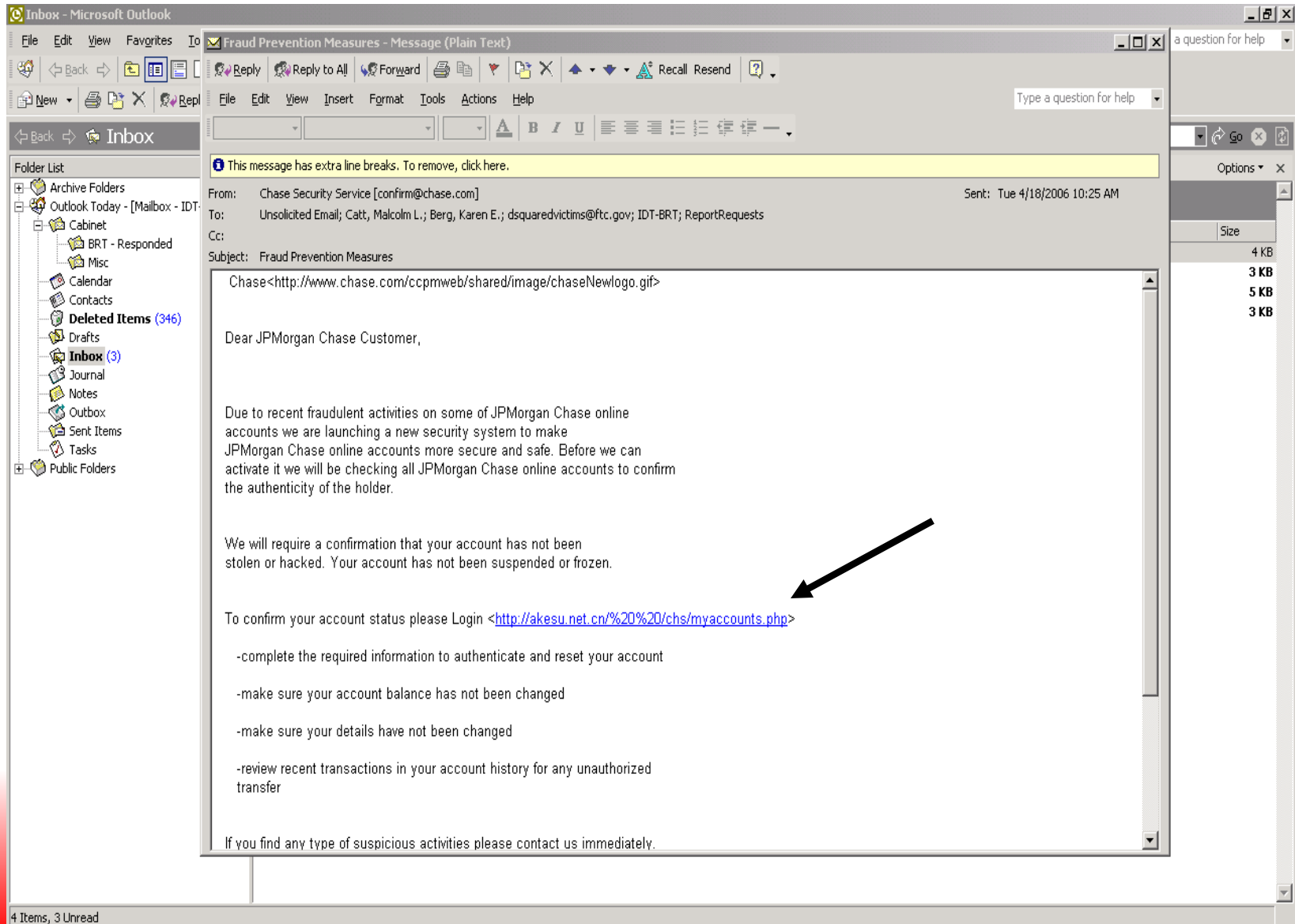
Shoulder Surfing



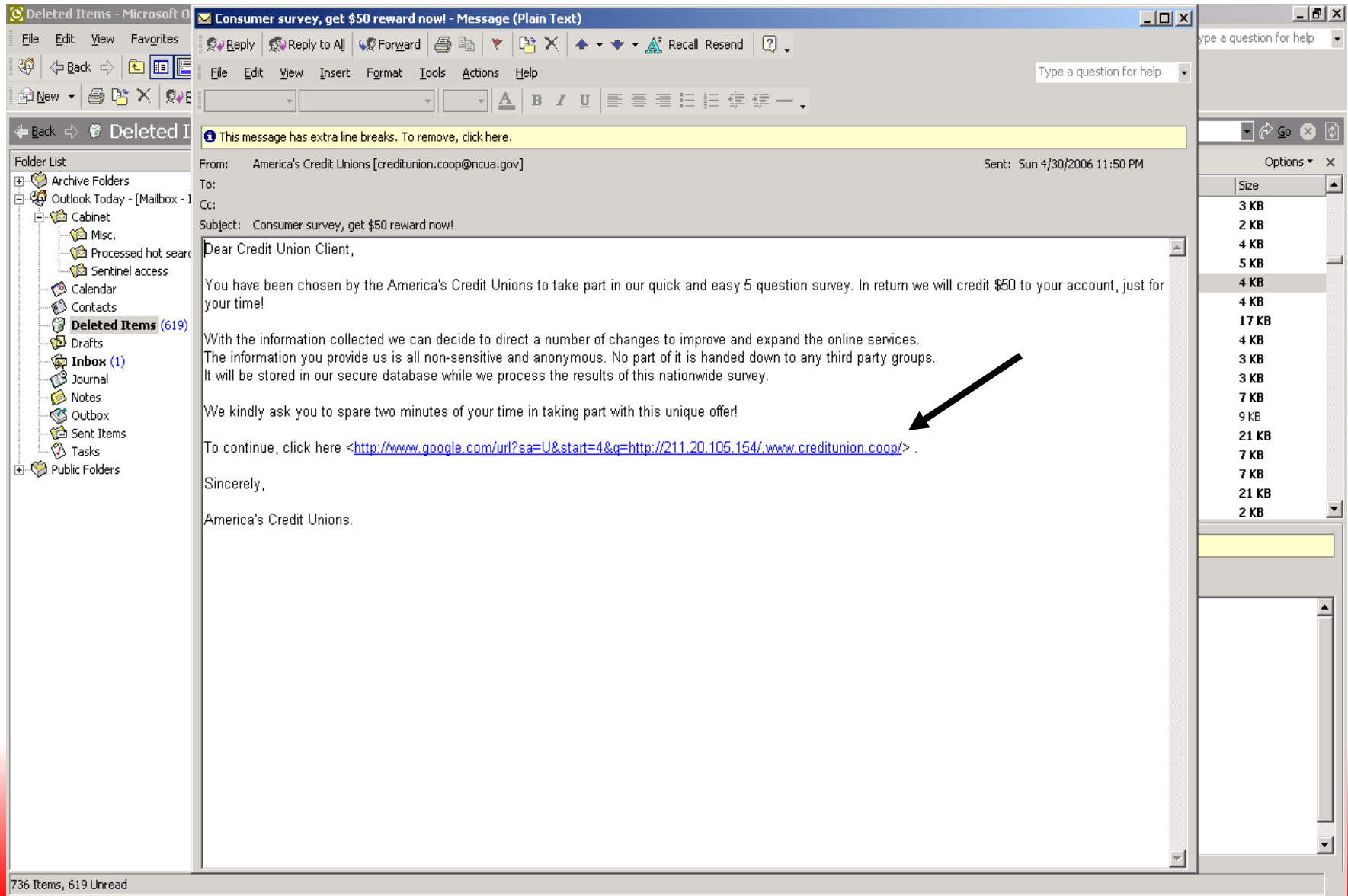
Skimming



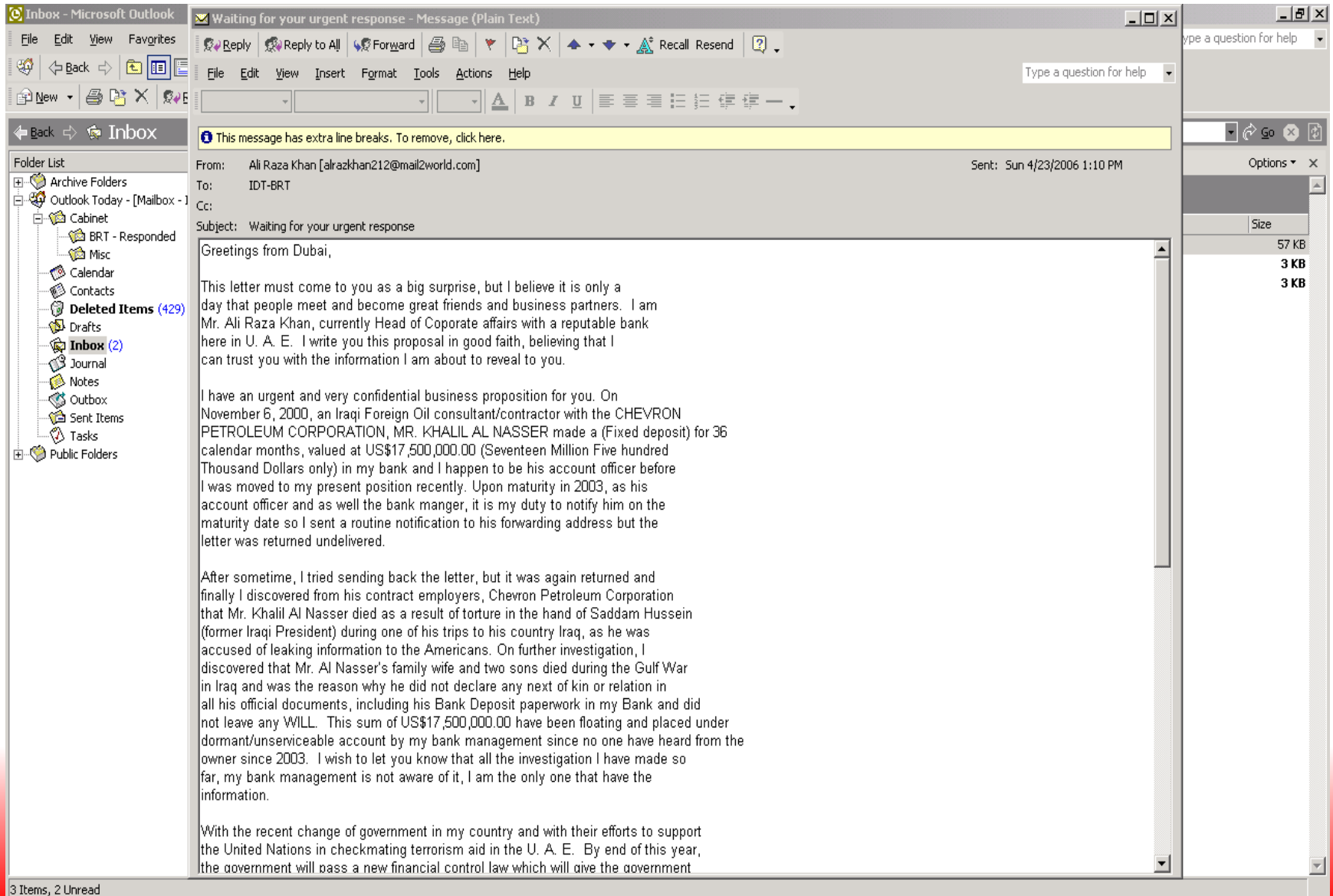
Phishing



Phishing



Phishing



Consequences of Identity Theft

- ◆ Identity thief seldom pays bills for debts incurred under your name
- ◆ You may not discover for months or years
- ◆ You are then saddled with bad credit report
- ◆ Due to bad credit report, you may be denied new credit, loans, mortgages, utility service, or employment
- ◆ Where criminal record created in your name, you may fail background checks for employment, firearms, etc., may even spend time in jail

Identity Theft and Assumption Deterrence Act of 1998

- ◆ Responded to widespread incidence of identity theft
- ◆ Recognizes non-monetary harm suffered by individual victims as well as monetary harm suffered by financial institutions
- ◆ Recognizes personal information, not just personal documents, as a basis for fraud

Identity Theft and Assumption Deterrence Act of 1998

Under the ID Theft Act, the FTC is required to: *Establish a Centralized Complaint & Consumer Education Service, and*

- ◆ Create a database of victims' complaints
- ◆ Provide useful information to victims of identity theft
- ◆ Refer victims complaints to:
 - law enforcement agencies
 - credit bureaus, appropriate entities

Core Components of FTC's Identity Theft Program

- ◆ **Toll-free phone number for victims
1-877-ID THEFT (438-4338)**

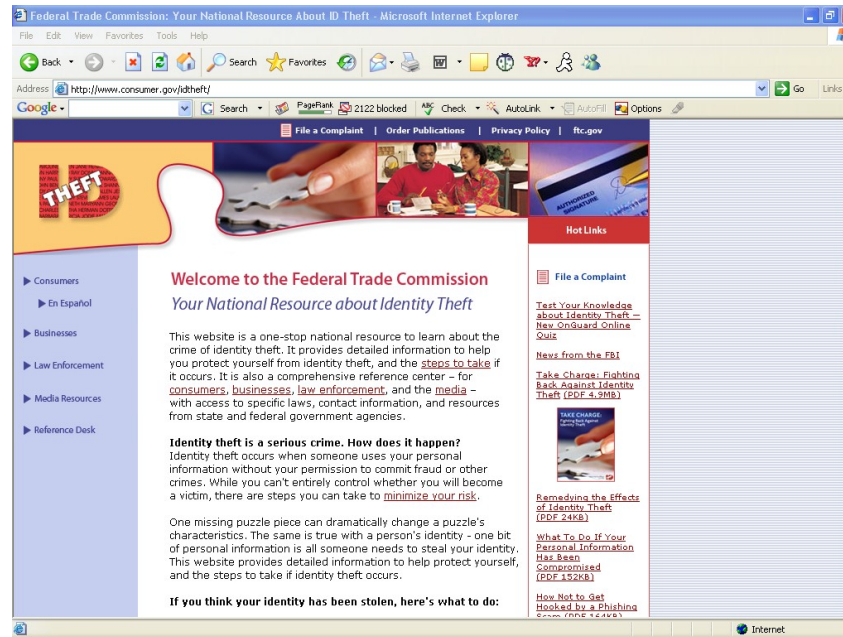
- Inform consumers:

- ❖ how to minimize risks (100% prevention not attainable)
- ❖ what first steps to take to recover
- ❖ what their rights are, what is possible
- ❖ subsequent steps, referrals to other resources

Core Components of FTC's Identity Theft Program

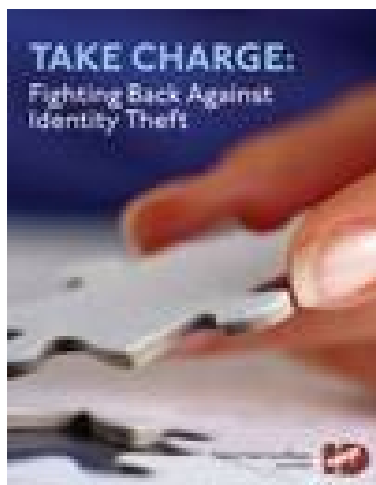
• www.consumer.gov/idtheft

• Online Complaint Form
• ID Theft Affidavit Online



Core Components of FTC's Identity Theft Program

- ◆ Take Charge: Fighting Back Against Identity Theft
- ◆ ID Theft: What It's All About



Core Components of FTC's Identity Theft Program

- ◆ Identity Theft Data Clearinghouse
 - Consumer Sentinel Access
 - Case Referral Program

What the Clearinghouse Shows About ID Theft

- ◆ Data from first 5 years of operation analyzed for broad trends and patterns
- ◆ Over 1,000,000 complaints as of April 2006.
 - Currently receiving over 15,000 calls per week.
 - Sources: Hotline, Online Complaint Form, Mail, SSA-OIG Fraud Hotline, ITAC, and Law Enforcement

Figure 5



IDENTITY THEFT
Data Clearinghouse



How Victims' Information is Misused¹ Calendar Years 2003 through 2005

Credit Card Fraud

	Percentages	Percentages	Percentages
Theft Subtype	CY-2003	CY-2004	CY-2005
New Accounts	19.3%	16.5%	15.6%
Existing Account	12.0%	11.9%	11.3%
Unspecified	1.4%	0.1%	0.2%
Total	32%	28%	26%

Phone or Utilities Fraud

	Percentages	Percentages	Percentages
Theft Subtype	CY-2003	CY-2004	CY-2005
Wireless - New Accounts	10.5%	10.0%	9.0%
Telephone - New Accounts	5.7%	6.0%	5.5%
Utilities - New Accounts	3.9%	4.3%	5.2%
Unauthorized Charges to Existing Accounts	0.6%	0.7%	0.7%
Unspecified	0.8%	0.3%	0.4%
Total	20%	19%	18%

Bank Fraud²

	Percentages	Percentages	Percentages
Theft Subtype	CY-2003	CY-2004	CY-2005
Electronic Fund Transfer	4.8%	6.6%	7.9%
Existing Accounts	8.3%	8.5%	7.4%
New Accounts	3.8%	3.6%	3.3%
Unspecified	0.5%	0.1%	0.1%
Total	17%	18%	17%

Employment-Related Fraud

	Percentages	Percentages	Percentages
Theft Subtype	CY-2003	CY-2004	CY-2005
Employment-Related Fraud	11%	13%	12%

Attempted Identity Theft

	Percentages	Percentages	Percentages
Theft Subtype	CY-2003	CY-2004	CY-2005
Attempted Identity Theft	8%	6%	6%

Government Documents or Benefits Fraud

	Percentages	Percentages	Percentages
Theft Subtype	CY-2003	CY-2004	CY-2005
Fraudulent Tax Return Filed	3.7%	3.9%	4.7%
Driver's License Issued / Forged	2.3%	2.3%	1.8%
Government Benefits Applied For / Received	1.3%	1.4%	1.5%
Other Government Documents Issued / Forged	0.4%	0.7%	0.6%
Social Security Card Issued / Forged	0.4%	0.5%	0.3%
Unspecified	<0.1%	<0.1%	<0.1%
Total	8%	8%	9%

Loan Fraud

	Percentages	Percentages	Percentages
Theft Subtype	CY-2003	CY-2004	CY-2005
Business / Personal / Student Loan	2.3%	2.6%	2.6%
Auto Loan / Lease	2.0%	1.9%	1.8%
Real Estate Loan	1.0%	1.2%	1.2%
Unspecified	0.3%	0.2%	0.2%
Total	5%	5%	5%

Other Identity Theft

	Percentages	Percentages	Percentages
Theft Subtype	CY-2003	CY-2004	CY-2005
Evasion of Legal Sanctions	2.1%	2.4%	2.2%
Internet / E-mail	1.6%	1.8%	1.9%
Medical	1.8%	1.8%	1.8%
Apartment / House Rented	0.9%	0.9%	0.9%
Insurance	0.3%	0.4%	0.4%
Property Rental Fraud	0.2%	0.3%	0.3%
Bankruptcy	0.3%	0.3%	0.3%
Child Support	0.2%	0.3%	0.2%
Magazines	0.1%	0.2%	0.2%
Securities / Other Investments	0.2%	0.1%	0.2%
Other	11.6%	14.4%	17.6%
Total	19%	22%	25%

¹Percentages are based on the total number of complaints in the Identity Theft Data Clearinghouse for each calendar year:

CY-2003 = 215,177; CY-2004 = 246,847; and CY-2005 = 255,565. Note that 20% of identity theft complaints include more than one type of identity theft in CY-2005, 19% and 20% for CY-2003 and CY-2004, respectively.



Figure 7a

Major Metropolitan Areas Ranking for Identity Theft - Related

Rank	Metropolitan Area	Complaints	Complaints Per 100,000 Population	Rank	Metropolitan Area	Complaints	Complaints Per 100,000 Population
1	Phoenix-Mesa-Scottsdale, AZ MSA	6,406	178.3	26	Indianapolis, IN MSA	1,408	88.3
2	Las Vegas-Paradise, NV MSA	2,499	158.5	27	Salt Lake City, UT MSA	887	88.2
3	Riverside-San Bernardino-Ontario, CA MSA	5,308	145.7	28	Oklahoma City, OK MSA	988	87.2
4	Dallas-Fort Worth-Arlington, TX MSA	7,892	141.2	29	Philadelphia-Camden-Wilmington, PA-NJ-DE-MD MSA	4,965	86.0
5	Los Angeles-Long Beach-Santa Ana, CA MSA	17,312	134.9	30	Jacksonville, FL MSA	1,025	85.2
6	Miami-Fort Lauderdale-Miami Beach, FL MSA	6,967	131.7	31	Baltimore-Towson, MD MSA	2,173	83.1
7	San Francisco-Oakland-Fremont, CA MSA	5,433	130.7	32	Cleveland-Elyria-Mentor, OH MSA	1,760	82.3
8	Houston-Baytown-Sugar Land, TX MSA	6,502	128.1	33	Kansas City, MO-KS MSA	1,567	82.3
9	San Diego-Carlsbad-San Marcos, CA MSA	3,559	121.4	34	New Orleans-Metairie-Kenner, LA MSA	1,069	81.1
10	San Antonio, TX MSA	2,168	119.1	35	Milwaukee-Waukesha-West Allis, WI MSA	1,141	75.3
11	Denver-Aurora, CO MSA	2,704	117.5	36	Minneapolis-St. Paul-Bloomington, MN-WI MSA	2,307	74.8
12	Atlanta-Sandy Springs-Marietta, GA MSA	5,417	117.5	37	Birmingham-Hoover, AL MSA	787	73.4
13	Orlando, FL MSA	2,084	115.6	38	St. Louis, MO-IL MSA	1,997	73.0
14	Sacramento--Arden-Arcade-Roseville, CA MSA	2,250	113.9	39	Columbus, OH MSA	1,218	72.7
15	Seattle-Tacoma-Bellevue, WA MSA	3,385	107.7	40	Virginia Beach-Norfolk-Newport News, VA-NC MSA	1,117	68.2
16	Washington-Arlington-Alexandria, DC-VA-MD-WV MSA	5,457	107.2	41	Richmond, VA MSA	771	67.7
17	Charlotte-Gastonia-Concord, NC-SC MSA	1,498	104.2	42	Rochester, NY MSA	663	63.7
18	San Jose-Sunnyvale-Santa Clara, CA MSA	1,779	102.6	43	Nashville-Davidson--Murfreesboro, TN MSA	872	63.6
19	Chicago-Naperville-Joliet, IL-IN-WI MSA	9,534	102.1	44	Boston-Cambridge-Quincy, MA-NH MSA	2,816	63.4
20	Austin-Round Rock, TX MSA	1,389	100.8	45	Buffalo-Niagara Falls, NY MSA	733	63.2
21	New York-Northern New Jersey-Long Island, NY-NJ-PA MSA	18,457	99.0	46	Hartford-West Hartford-East Hartford, CT MSA	736	62.5
22	Portland-Vancouver-Beaverton, OR-WA MSA	1,932	94.7	47	Cincinnati-Middletown, OH-KY-IN MSA	1,134	55.4
23	Detroit-Warren-Livonia, MI MSA	4,124	92.0	48	Providence-New Bedford-Fall River, RI-MA MSA	895	55.1
24	Memphis, TN-MS-AR MSA	1,131	91.3	49	Louisville, KY-IN MSA	656	55.1
25	Tampa-St. Petersburg-Clearwater, FL MSA	2,307	91.1	50	Pittsburgh, PA MSA	1,176	48.8

¹Ranking is based on the number of identity theft complaints per 100,000 inhabitants for each metropolitan area. This chart illustrates major Metropolitan Statistical Areas (MSA) with a population of one million or more. Metropolitan areas presented here are those defined by the Office of Management and Budget (OMB) as of December 2003 (www.census.gov/population/www/estimates/metropop/PopTable01.xls).



Figure 7b

Identity Theft Victims by State (Per 100,000 Population)¹

		<i>January 1</i>		<i>December 31, 2005</i>			
Rank	Victim State	Victims Per 100,000 Population	Number of Victims	Rank	Victim State	Victims Per 100,000 Population	Number of Victims
1	Arizona	156.9	9,320	26	Alaska	63.4	421
2	Nevada	130.2	3,144	27	Louisiana	62.6	2,831
3	California	125.0	45,175	28	Massachusetts	62.5	3,999
4	Texas	116.5	26,624	29	Ohio	62.4	7,155
5	Colorado	97.2	4,535	30	Minnesota	58.7	3,015
6	Florida	95.8	17,048	31	Alabama	58.7	2,675
7	Washington	92.4	5,810	32	Kansas	58.5	1,606
8	New York	90.3	17,387	33	Arkansas	58.2	1,617
9	Georgia	87.3	7,918	34	Rhode Island	58.2	626
10	Illinois	87.3	11,137	35	Tennessee	57.2	3,412
11	Maryland	86.6	4,848	36	South Carolina	56.8	2,416
12	New Mexico	84.7	1,634	37	Nebraska	52.3	919
13	Oregon	81.7	2,973	38	Idaho	52.1	745
14	New Jersey	75.5	6,582	39	Wisconsin	50.3	2,782
15	Michigan	70.5	7,139	40	Mississippi	49.9	1,458
16	Delaware	69.1	583	41	New Hampshire	49.2	645
17	Virginia	68.2	5,163	42	Wyoming	44.0	224
18	Oklahoma	67.7	2,403	43	Kentucky	43.5	1,815
19	Missouri	67.6	3,920	44	Montana	42.5	398
20	Utah	67.5	1,668	45	West Virginia	37.3	677
21	North Carolina	67.1	5,830	46	Maine	37.2	491
22	Indiana	67.0	4,201	47	Iowa	36.7	1,090
23	Connecticut	65.9	2,313	48	Vermont	32.3	201
24	Pennsylvania	63.6	7,908	49	South Dakota	30.0	233
25	Hawaii	63.5	810	50	North Dakota	24.8	158

¹Per 100,000 unit of population estimates are based on the 2005 U.S. Census population estimates (Table NST-EST2005-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico: April 1, 2000 to July 1, 2005). Numbers for the District of Columbia are 842 victims and 152.9 victims per 100,000 population.

FTC's Identity Theft Survey

- ◆ Released September 3, 2003
 - ❖ 3.23 million Victims found that a new account was opened in the past year.
 - ❖ 9.91 million total Victims in the past year and 27.3 million in the last 5 years.
 - ❖ \$47.6 billion was lost by businesses, including Financial Institutions due to the identity thief.
 - ❖ \$5.0 billion was spent by victims to resolve the theft.

State Laws

- ◆ District of Columbia:
 - Identity Theft Statute (2004, Title 22 Section 3227)
 - ❖ Makes IDT a criminal offense
 - ❖ Requires the Metropolitan Police to take a report and provide a copy of the report to the victim.
- ◆ Maryland:
 - Identity Theft Statute
 - ❖ Makes IDT a criminal offense
 - ❖ Requires local law enforcement to take a report and provide a copy of the report to the victim (2005 H.B. 800)

State Laws

- ◆ Virginia
 - Identity Theft statute (18.2-186.3)
 - ◆ Makes IDT a criminal offense

How Can You Protect Yourself from ID Theft?

- ◆ Today:
 - Order your credit reports – review carefully
 - Put passwords on your accounts
 - ❖ Strong passwords – **not** Mothers Maiden Name
 - Secure your personal information in your home from others (roommates, employees)
 - Ask about security procedures in your workplace

Other Steps You Can Take To Prevent Identity Theft

◆ Ongoing Basis:

- Order your credit report every year (www.annualcreditreport.com or 1-877-322-8228)
- Do not provide personal information over the phone, Internet, or through the mail
- Guard mail and trash from theft
- Pay attention to billing cycles
- Opt out of pre-approved credit card offers (1-888-567-8688)
- Be wary of promotional scams
- Keep your virus protection software updated

What Should Victims Do?

- ◆ Immediately:
 - Call the Credit Reporting Agencies (CRAs) and have a fraud alert placed on your credit report.
 - Contact creditors' fraud departments, report fraudulent accounts and charges
 - File a Police Report with your local department and get a copy of it. Be persistent if necessary
 - File a complaint with the Federal Trade Commission

Welcome to Military Sentinel - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Search Favorites Media Print Copy Paste

Address <http://www.consumer.gov/military/> Go

Links Customize Links Free AOL & Unlimited Internet Free Hotmail RealPlayer Windows



Military Sentinel

U.S. Army U.S. Marines U.S. Navy U.S. Air Force FTC

FILE COMPLAINT

'Active Duty' Alerts Help Protect Military Personnel from Identity Theft

[\[TXT\]](#) [\[PDF\]](#)

New Department of Defense's "Financial Readiness Campaign" Partner Web Site

The new site, www.militarymoney.com, was created to highlight specific financial issues and challenge affecting service members and their families. The site includes the Military Money Minute. A new daily 60 second spot on the Armed Forces Radio Network, delivering savvy advice on issues from military tax breaks to financial scams and more.

FTC Announces Complaint Referral Program with Credit Bureaus

Financial Literacy Information

The FTC, the Better Business Bureau, AARP, NAAO and other partners have pooled their materials

Welcome to Military Sentinel

Military Sentinel is a project of the Federal Trade Commission and the Department of Defense to identify and target consumer protection issues that affect members of the United States Armed Forces and their families.

To file a consumer complaint, click on your service seal. This will link you to the consumer complaint forms.

Military Sentinel also provides a gateway to consumer education materials covering a wide range of consumer protection issues, from auto leasing, to identity theft, to work-at-home scams.

To view consumer education material and find out more about the Federal Trade Commission, click on the Federal Trade Commission seal.

Military Sentinel allows members of the United States Armed Forces to enter consumer complaints directly into a database that is immediately accessible by over 500 law enforcement organizations throughout the United States, Canada, and Australia. These law enforcement agencies use this complaint data to target cases for prosecution and other enforcement measures. The information from **Military Sentinel** can also be used by members of the JAG staff and others in the Department of Defense to help protect armed services members and their families from consumer protection-related problems.

Local intranet

Next Steps for Victims

- ◆ Notify each credit reporting agency of all of the inaccuracies on your credit reports, including Inquiries. Call and follow up *in writing*.
- ◆ Notify each creditor where the identity thief committed fraud *in writing*.
- ◆ Get creditors to provide you something *in writing* stating they have closed the accounts and absolved you of the fraudulent debts

Fair and Accurate Credit Transactions Act (FACTA)

- ◆ Amended the Fair Credit Reporting Act
- ◆ Signed into law in December 4, 2003
- ◆ Provided many new legal rights to victims of identity theft

New Resolution Tools and Initiatives for Consumers

Identity Theft Report Block

If Victim Provides CRAs with Police/IDT Report:

- ◆ CRAs will automatically block inaccurate information on victim's credit report, notify creditors who furnished

One Call Fraud Alert

If Victim Reports to One CRA:

First CRA contacted will share information with the other two; each company will post a fraud alert on and mail the victim a copy of their credit file

Active Duty Alert

- ◆ If you are a member of the military and away from your usual duty station, you may place an “Active Duty” alert on your credit file.
- ◆ The alerts last 1 year but can be renewed.

Fair Credit Reporting Act

- ◆ Section 609(e):
 - Victims and Law Enforcement can get identity theft related transaction records from businesses *without a subpoena*
 - ❖ Victims must provide proof of identity
 - ❖ Victims must provide a **POLICE REPORT** and a completed affidavit
 - ❖ Became effective June 2, 2004

Fair Credit Reporting Act

- ◆ Section 615(g)
 - Victims and Law Enforcement can get identity theft related transaction records from third party debt collectors *without a subpoena*
 - ❖ Victims must provide proof of identity
 - ❖ Victims must provide a **POLICE REPORT** and a completed affidavit
 - ❖ Became effective December 3, 2004

SUMMARY: PROVING YOU ARE A VICTIM

- ◆ Get Police Report; send to CRAs, attach to Affidavit
- ◆ Complete ID Theft Affidavit or other fraud packets; send to creditors
- ◆ Get creditors to provide you resolution letters
- ◆ Organize your documents, keep copies

BUSINESS BEST PRACTICES

Safeguarding Information

- ◆ Written Security Plan
 - Designate someone to coordinate information security program
 - Identify and assess risks to employee/customer data
 - Design and implement a safeguards program

Securing Information

- ◆ Via Employee Management & Training
- ◆ Via Information Systems
- ◆ Via Detecting and Managing System Failures

Employee Management & Training

- ◆ Limit access of data to employees who have a business reason to see it
- ◆ Control access to sensitive information by requiring “strong” passwords that must be changed regularly
- ◆ Develop policies to protect laptops, PDAs, cell phones and other mobile devices

Employee Management & Training (cont'd)

- ◆ Train employees to take simple steps to protect information
 - Locking rooms and file cabinets
 - Not posting employee passwords in easily to find places
 - Encrypting sensitive information when it's transmitted electronically

Employee Management & Training (cont'd)

- ◆ Prevent terminated employees from accessing information by shutting down their access to data

Information Systems

- ◆ Includes network and software design, and information processing, storage, transmission, retrieval, and disposal

Information Systems (cont'd)

- ◆ Know where sensitive data is stored
 - Store records in a room or cabinet that is locked
 - When stored on a server or other computer, ensure that the computer is accessible only with a “strong” password
 - When possible, avoid storing sensitive data on a computer with an internet connection
 - Maintain secure backup records and a careful inventory of computers and equipment that store this information

Information Systems (cont'd)

- ◆ Dispose of information in a secure way
 - Consider having a designated person in charge of disposal of records.
 - If an outside company is used, be sure to do due diligence and monitoring
 - Burn, pulverize or shred
 - Destroy or erase data when disposing of computers, disks, CD, hard drivers, etc.

Detecting & Managing System Failures

- ◆ Maintain:
 - Check with software vendors and install appropriate patches
 - Use anti-virus and anti-spy software
 - Maintain an up to date firewall

Detecting & Managing System Failures (cont'd)

- ◆ Oversight and Audit:
 - Keep logs of activity on your network and continuously monitor for unauthorized access
 - Use an up to date intrusion detection system
 - Monitor both in and out bound transfers of information, especially for unexpectedly large amounts of data being transmitted

Detecting & Managing System Failures (cont'd)

- ◆ If a breach occurs:
 - Take immediate action to secure any information that has or may have been compromised
 - Preserve and review files or programs that may reveal how the breach occurred
 - Consider notifying consumers/employees, law enforcement

Detecting & Managing System Failures (cont'd)

◆ Notification:

- Notifying employees enables them to take steps to prevent or limit harm of identity theft
- Notifying criminal law enforcement promotes investigation and prosecution

Recent Breach

Pentagon Hacker Compromises Personal Data - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.washingtonpost.com/wp-dyn/content/article/2006/04/28/AR2006042801540.html>

Links [Customize Links](#) [Free AOL & Unlimited Internet](#) [Free Hotmail](#) [RealPlayer](#) [Windows](#)

[Print This Article](#)
[E-Mail This Article](#)
[Subscribe to The Post](#)

Advertisement


Pentagon Hacker Compromises Personal Data

By ROBERT BURNS
The Associated Press
Friday, April 28, 2006; 5:19 PM

WASHINGTON -- An intruder gained access to a Defense Department computer server and compromised confidential health care insurance information for more than 14,000 people, the department said Friday.

William Winkenwerder Jr., the assistant defense secretary for health affairs, said the affected individuals have been advised by letter that the compromise of personal information could put them at risk for identity theft.

"Such incidents are reprehensible, and we deeply regret the inconvenience this may cause the people we serve," he said in a brief statement.

The Pentagon established a toll-free telephone number (1-800-600-9332) for affected people to call if they have questions. The computer server is for people insured under the Pentagon's TRICARE health care system.

The type of information that was compromised was not disclosed in the Pentagon announcement, but Winkenwerder said it varied and investigators do not know the intent of the crime or if the compromised information will be misused.

A spokesman for Winkenwerder, who asked not to be identified, said the

Advertisement
[Click Here](#)

TOP JOBS FROM LOCAL EMPLOYERS

[Deputy Associate Cio](#) / IRS
[Executive Director](#) / CONFIDENTIAL LISTING
[Regional Radio Executive, Division II](#) / AP BROADCAST
[Sales](#) / WE HAVE LOANS 4 U
[Staff Accountant](#) / SIM-G TECHNOLOGIES
[All Top Jobs](#)

FEATURED ADVERTISER LINKS

[Refinance Rates As Low As 2.9% - FREE QUOTES](#)
[For College Graduates, Reduce Your Student Loans](#)
[Seating Charts, Tim McGraw Tickets w/ Faith Hill, Pavarotti Tickets, NASCAR Tickets](#)
[ReNu Vision Loss Danger - New Cases Just Reported](#)
[\\$145,000 Mortgage for Under \\$484/Month!](#)
[Get a \\$200,000 loan for \\$833/Month](#)
[Promotional Pens, T-shirts, Custom Hats](#)
[Have a Business to Buy or Sell -- Learn How](#)
[Cool Gadgets, Great Deals, Visit CircuitCity.com](#)
[Earn a free trip on Acela. Learn more.](#)
[Get Free Checking with direct deposit](#)
[Secure Your Passwords, One-click logins - RoboForm](#)

WHO'S BLOGGING?

Read what bloggers are saying about this article.
• [Google News' Journal](#)
[Full List of Blogs \(1 links\)](#)
Most Blogged About Articles
[On washingtonpost.com](#) | [On the web](#)
POWERED BY
Technorati

SAVE & SHARE

• [Tag This Article](#)
• [Saving options](#)
Powered by [Del.icio.us](#)

MOST VIEWED ARTICLES

Nation On the Site
Updated 4:46 p.m. ET

- [States sue Bush over fuel efficiency](#)
- [FBI Sought Data on Thousands in '05](#)
- [Justices Reinstate Smith's Claim](#)
- [Insurers Retreat From Coasts](#)
- [Polygraph Results Often in Question](#)

RSS NEWS FEEDS

[XML Top News](#)
[XML Nation](#)
[What is RSS?](#) | [All RSS Feeds](#)

E-MAIL NEWSLETTERS

View a Sample and Sign Up
• [Today's Headlines & Columnists](#)
• [Daily Politics News & Analysis](#)

Error on page.

Internet

Even More Recent...

Thieves Steal Personal Data of 26.5M Vets - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print

Address <http://www.washingtonpost.com/wp-dyn/content/article/2006/05/22/AR2006052200839.html> Go

Links Customize Links Free AOL & Unlimited Internet Free Hotmail RealPlayer Windows

washingtonpost.com > Technology > Special Reports > Privacy

Thieves Steal Personal Data of 26.5M Vets

By HOPE YEN
The Associated Press
Tuesday, May 23, 2006; 2:23 AM

WASHINGTON -- Thieves took sensitive personal information on 26.5 million U.S. veterans, including Social Security numbers and birth dates, after a Veterans Affairs employee improperly brought the material home, the government said Monday.

The information involved mainly those veterans who served and have been discharged since 1975, said VA Secretary Jim Nicholson. Data of veterans discharged before 1975 who submitted claims to the agency may have been included.

Nicholson said there was no evidence the thieves had used the data for identity theft, and an investigation was continuing.

"It's highly probable that they do not know what they have," he said in a briefing with reporters. "We have decided that we must exercise an abundance of caution and make sure our veterans are aware of this incident."

Veterans advocates expressed alarm.

[Enlarge This Photo](#)



Symbol of Veteran Affairs Dept. Personal data, including Social Security numbers of 26.5 million U.S. veterans, was stolen from a Veterans Affairs employee after he took the information home without authorization, the department said Monday, May 22, 2006. (AP Graphic)

Advertisement

[Click Here](#)

TOP JOBS FROM LOCAL EMPLOYERS

[Senior Accountant](#) / EATON AEROSPACE
[Welder](#) / S/WALES AEROSPACE
[Sped Teacher / Teaching Asst](#) / NOT LISTED
[Web Developer](#) / BOATU.S.
[Medical Billing Manager](#) / TIMOTHY J MALONE MD PC

[All Top Jobs](#)

FEATURED ADVERTISER LINKS

[Refinance Rates As Low As 2.9% - FREE QUOTES!](#)
[\\$40,000 for \\$277/mo. Fixed Rate Home Equity Loan](#)
[For College Graduates, Reduce Your Student Loans](#)
[Seating Charts, Tim McGraw Tickets w/ Faith Hill, Pavarotti Tickets, NASCAR Tickets](#)
[ReNu Lawsuit, Otho Ewa, Benzene, Advair, Crestor](#)
[\\$145,000 Mortgage for Under \\$484/Month!](#)
[Promotional Pens, T-shirts, Custom Hats](#)
[Cool Gadgets, Great Deals, Visit CircuitCity.com](#)
[Get Free Checking with direct deposit](#)

QUICK QUOTES

Enter Symbol [go](#)
[Tables](#) | [Portfolio](#) | [Index](#)

MOST VIEWED ARTICLES

Technology On the Site
Updated 9:31 a.m. ET

- [VA Data in Format Not Widely Used](#)
- [Microsoft Enters PC Security Market](#)
- [Sleuths Crack Tracking Code Discovered in Color Printers](#)
- [New Vehicle for Dissent Is a Fast Track to Prison](#)
- [Personal Data on Veterans Is Stolen](#)

RSS NEWS FEEDS

[XML Top News](#)
[XML Technology](#)
[What is RSS?](#) | [All RSS Feeds](#)

E-MAIL NEWSLETTERS

Error on page.

Internet

Publications

- ◆ Financial Institutions and Customer Information: Complying with the Safeguards Rule -

<http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm>

- ◆ Information Compromise and the Risk of Identity Theft: Guidance for Your Business -

<http://www.ftc.gov/bcp/online/pubs/buspubs/identityrespond.htm>

Contact Information:

Kathleen Claffie

202-326-3888

kclaffie@ftc.gov

Law Enforcement

FTC's Complaint Database

Identity Theft Data Clearinghouse

- ◆ Federal government's centralized database of identity theft victim complaints
 - Available **free** of cost over Consumer Sentinel
- ◆ Contents
 - victim contact information
 - suspect information: name, address, phone, relationship to the victim
 - description of crime, details
 - what financial institutions were involved
 - police report number, department name, contact information

Assist Law Enforcement Actions:

Multiplier Effect

- ◆ FTC's complaint information shared with local, state and federal law enforcement through: **CONSUMER SENTINEL**
 - Real-time, desktop access through a secure website
 - Coordinate cross-jurisdictional investigations with "ALERTS" function
 - Track particular complaints or patterns with "AUTO-QUERY"
 - Case Referral Program – Quarterly Mining & Analysis – refer out largest cases

Uses of IDT Data Clearinghouse

Initiate New Investigations

- ◆ **Find clusters of victims that report same suspect name, address or phone**
- ◆ **Additional addresses and phone numbers related to those leads**
- ◆ **Autoquery your zip codes, hot addresses**

Grow Ongoing Investigations

- ◆ Find additional complaints about suspect addresses, names, phone numbers
 - **Autoquery**
- ◆ Find additional defrauded companies

Assist in handling victim complaints

- ◆ Check for additional complaints relating to addresses and phone numbers reported by victim

Hot Searches

- ◆ For ongoing investigations, where LEOs are pressed for time, or have a complex search, request a “Hot Search” from the FTC ID Theft Team
- ◆ Send an email to idtsearch@ftc.gov
- ◆ Include your contact information and
 - Suspect contact/location information, or
 - Victim information



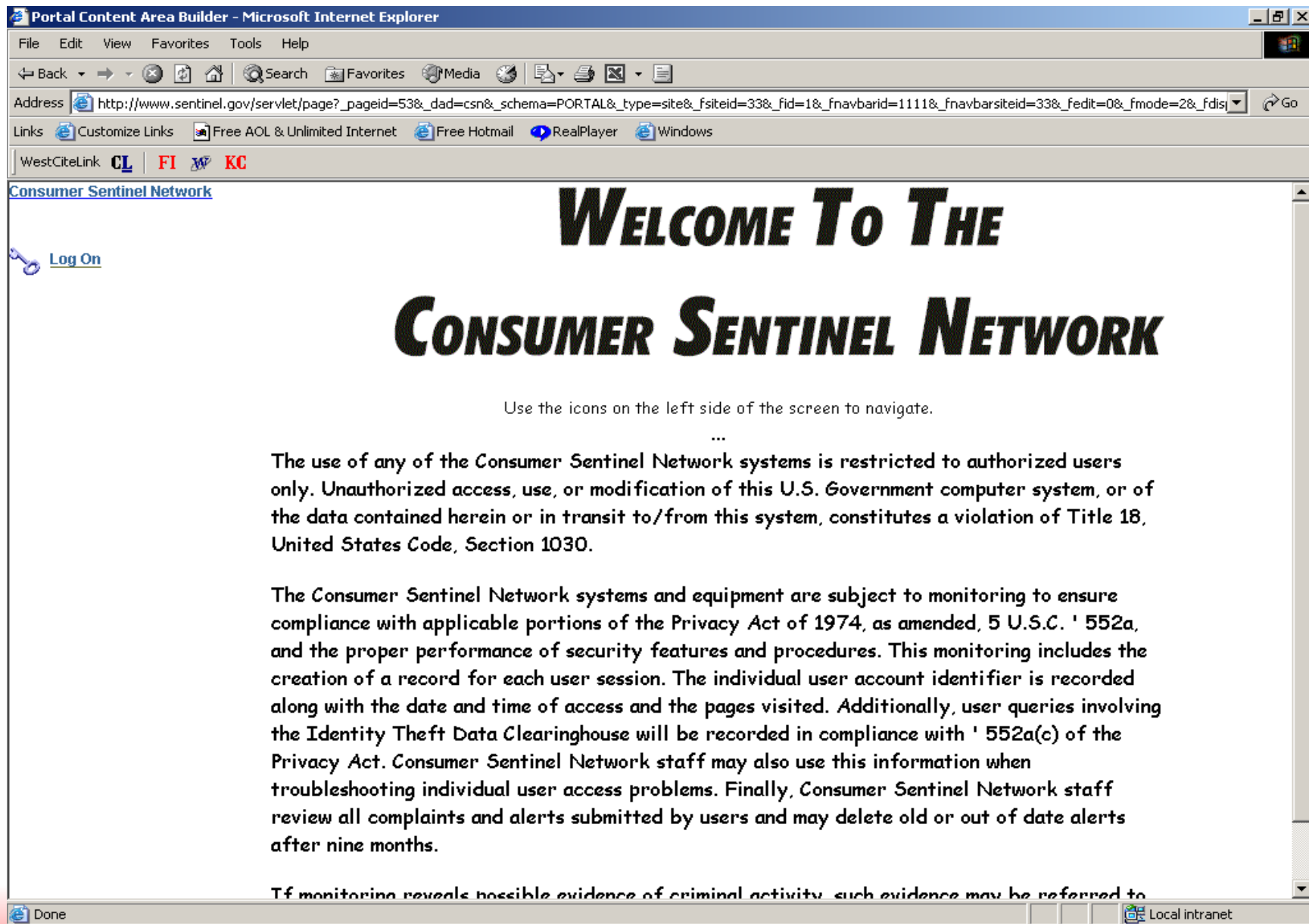
WARNING!!!

The use of this system is restricted to authorized users only. Unauthorized access, use, or modification of this U.S. Government computer system, or of the data contained herein or in transit to/from this system, constitutes a violation of Title 18, United States Code, Section 1030. These systems and equipment are subject to monitoring to ensure proper performance of applicable security features and procedures. Such monitoring may result in the acquisition, recording and analysis of data being communicated, transmitted, processed or stored in this system by a user. In particular, we monitor the identity of each person who accesses this system, as well as the date and time of their access. In addition, we review all complaints and alerts submitted by users. If monitoring reveals possible evidence of criminal activity, such evidence may be referred to appropriate law enforcement personnel for investigation and prosecution.

Use of this system is limited to law enforcement personnel whose agencies have entered into a [confidentiality agreement](#) with the Federal Trade Commission. Please remember that your use of the data contained in this system is limited by this confidentiality agreement.

CONTINUE

Last Update: Friday, April 25, 2003 12:10 PM



Portal Content Area Builder - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Copy Paste Address http://www.sentinel.gov/servlet/page?_pageid=55&_dad=csn&_schema=PORTAL&_type=site&_fsiteid=33&_fid=1&_fnavbarid=4435&_fnavbarsiteid=33&_fedit=0&_fmode=2&_fdis Links Customize Links Free AOL & Unlimited Internet Free Hotmail RealPlayer Windows WestCiteLink CL FI W KC

Consumer Sentinel Network

Welcome KCLAFFIE

Root Folder - Consumer Sentinel (Last Updated: 07-JAN-2005)

Log Off

CS Home

Complaints

Alerts

Orders/Actions

Contacts

Library

Tapes

Identity Theft

Military Sentinel

Consumer Planet

Q A Module

CIS

Do Not Call

WELCOME TO THE CONSUMER SENTINEL NETWORK

Use the icons on the left side of the screen to navigate.

...

The use of any of the Consumer Sentinel Network systems is restricted to authorized users only. Unauthorized access, use, or modification of this U.S. Government computer system, or of the data contained herein or in transit to/from this system, constitutes a violation of Title 18, United States Code, Section 1030.

The Consumer Sentinel Network systems and equipment are subject to monitoring to ensure compliance with applicable portions of the Privacy Act of 1974, as amended, 5 U.S.C. ' 552a, and the proper performance of security features and procedures. This monitoring includes the creation of a record for each user session. The individual user account identifier is recorded along with the date and time of access and the pages visited. Additionally, user queries involving the Identity Theft Data Clearinghouse will be recorded in compliance with ' 552a(c) of the Privacy Act. Consumer Sentinel Network staff may also use this information when troubleshooting individual user access problems. Finally, Consumer Sentinel Network staff review all complaints and alerts submitted by users and may delete old or out of date alerts after nine months

To --> [sentinel.gov](http://www.sentinel.gov)

Done Local intranet

Portal Content Area Builder - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Copy Paste Address http://www.sentinel.gov/servlet/page?_pageid=55&_dad=csn&_schema=PORTAL&_type=site&_fsiteid=33&_fid=1022&_fnavbarid=4435&_fnavbarsiteid=33&_fedit=0&_fmode=2& Go

Links Customize Links Free AOL & Unlimited Internet Free Hotmail RealPlayer Windows

WestCiteLink CL FI W KC

Consumer Sentinel Network

Log Off

CS Home
Complaints
Alerts
Orders/Actions
Contacts
Library
Tapes
Identity Theft
Military Sentinel
Consumer Planet
Q A Module
CIS
Do Not Call

ConsumerSentinel

IDENTITY THEFT
Data Clearinghouse

[Identity Theft Home Page](#)

Click on the hyperlink above, to access the "Identity Theft" page.

Search the Identity Theft Data Clearinghouse using additional features uniquely designed for reviewing identity theft data. Add your own identity theft complaints using special categories to capture the information.

[Consumer Sentinel Network : Identity Theft](#)

To --> [sentinel.gov](#)

Done Local intranet

How To Sign Up For Sentinel

- ◆ Confidentiality Agreement by head of your Department or Organization
 - Check list at www.consumer.gov/sentinel/members.htm
- ◆ Submit C.A. by Fax, (202) 326-3392
- ◆ Mail Hard Copy to FTC
- ◆ Approval in Two Weeks (*Approx.*)

How to Get a User ID & Password

- ◆ ***Individual User Application*** - signed by User and Supervisor
- ◆ Submit by Fax: 202-326-3392
- ◆ Mail Hard Copy to FTC
- ◆ Password and Log In/Security Tools arrive in 1-2 weeks (approx.)
- ◆ Questions? Call 877-701-9595

Joint USSS, FTC, AAMVA, DOJ, USPIIS Law Enforcement Training

- ◆ Identity Crime: an Interactive Resource Guide
 - Over 55,000 CD-ROMs distributed to state and local law enforcement
 - Launched in August 2003
- ◆ Law Enforcement Training Seminars
 - One day “how-to” seminars for state and local officers: investigating cases, successful prosecutions
 - 23 locations nationwide accomplished from 03/2002-05/2006



IDENTITY crime

United States Secret Service presents in a joint effort with the
Postal Inspection Service
Federal Trade Commission
International Association of Chiefs of Police



Contact Information:

Kathleen Claffie

202-326-3888

kclaffie@ftc.gov